What is an IDS?

An **Intrusion Detection System (IDS)** monitors network or system activity for malicious behaviour or policy violations. It analyses traffic and alerts administrators of potential threats, but doesn’t block them. It is helpful in mitigating attacks and helps increasing overall system security.

Types of IDS/IPS

* Network Based
  + Monitors & Examines network traffic for any suspicious activity / threats
  + Upon examining packets flowing, if detection is present, notification created
* Wireless Based
  + Analyzes traffic & wireless protocol activities over Wireless network
* Network Behaviour Based
  + Examines network traffic to identify threats generating unusual traffic flows
  + Eg : DDOS, Malware activity. Mostly deployed Intranet.
* Host Based
  + Monitors & identifies intrusions within a single host’s file system & network events.
  + Can detect System level attacks. Also helps in Load balancing.

Methodologies of IPS/IDS

* Anomaly based Methodology
  + These types of attack are used for detecting the unknown attacks
  + It detects malicious traffic based on normal network traffic pattern
  + The disadvantage of such method is that it generates high false alarm rate
* Signature based Methodology
  + Detect unknown attacks which are already predefined in the form of signature and are saved.
  + It compares the network packet from the database of signature which is already stored in the network.
* Stateful Protocol Analysis
  + Compares established profiles of how protocols should behave against the observed behavior
  + It uses information about connections between the hosts and compares it with the entries present in the state table
  + Its main advantage is that system can detect attacks from inside a network
* Hybrid based
  + It is the integration of two different intrusion detection system – anomaly and signature-based detectors.
  + Collects the output of both anomaly and signature-based detector and then calculates the attack probability.
  + Updates anomaly detector’s normal network model and also signature-based detectors rule set.
  + Calculates the final decision on the probability of an attack by using the collected outputs of the anomaly and signature-based detectors.

What is SNORT?

Snort is a free open-source intrusion detection system. It's a popular and powerful multi packet tool run by a lot of different people and companies. One of the Signature based Intrusion Detection and Prevention System.

SNORT Components

A blue and white text on a blue background

Description automatically generated

How does SNORT work?

A diagram of a computer process

Description automatically generated

SNORT Packet Flow

A diagram of a packet decoder

Description automatically generated

SNORT Modes

A blue screen with white text

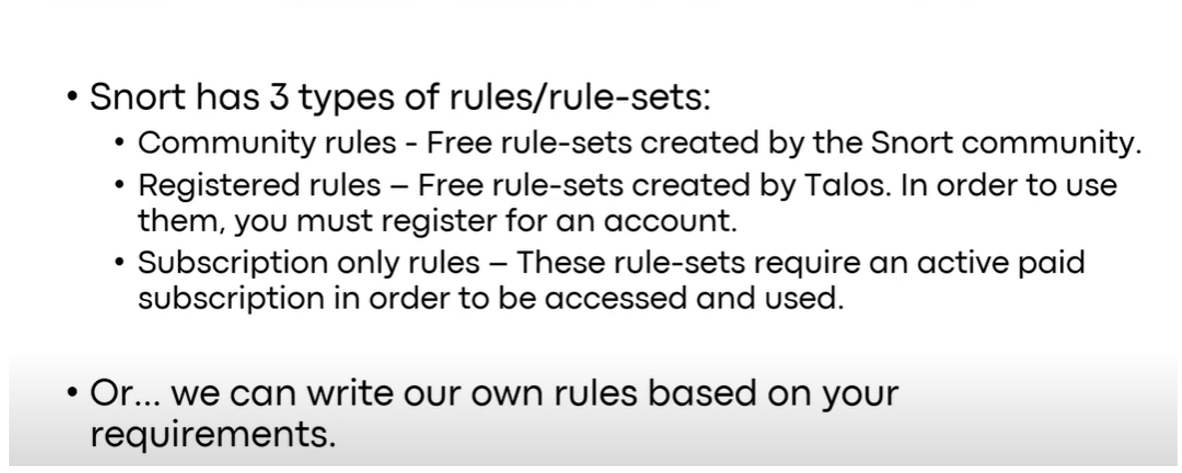
Description automatically generated

SNORT Protection

A blue screen with white text

Description automatically generated

SNORT RULES



A diagram of a computer program

Description automatically generated

A diagram of a network placement

Description automatically generated

A diagram of a network

Description automatically generated

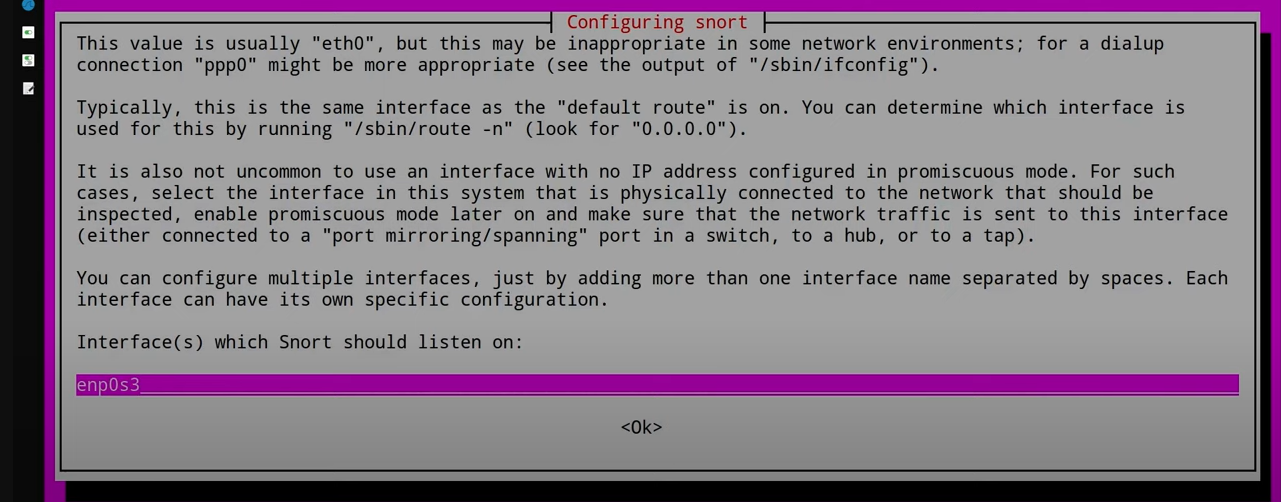
INSTALLING SNORT

We will now look at how we can install and run snort

Step1:Open your Ubuntu machine, go to terminal and type in

>sudo apt-get install snort -y

Then find and configure your interface as enp0s3 and the address range for your local area network.



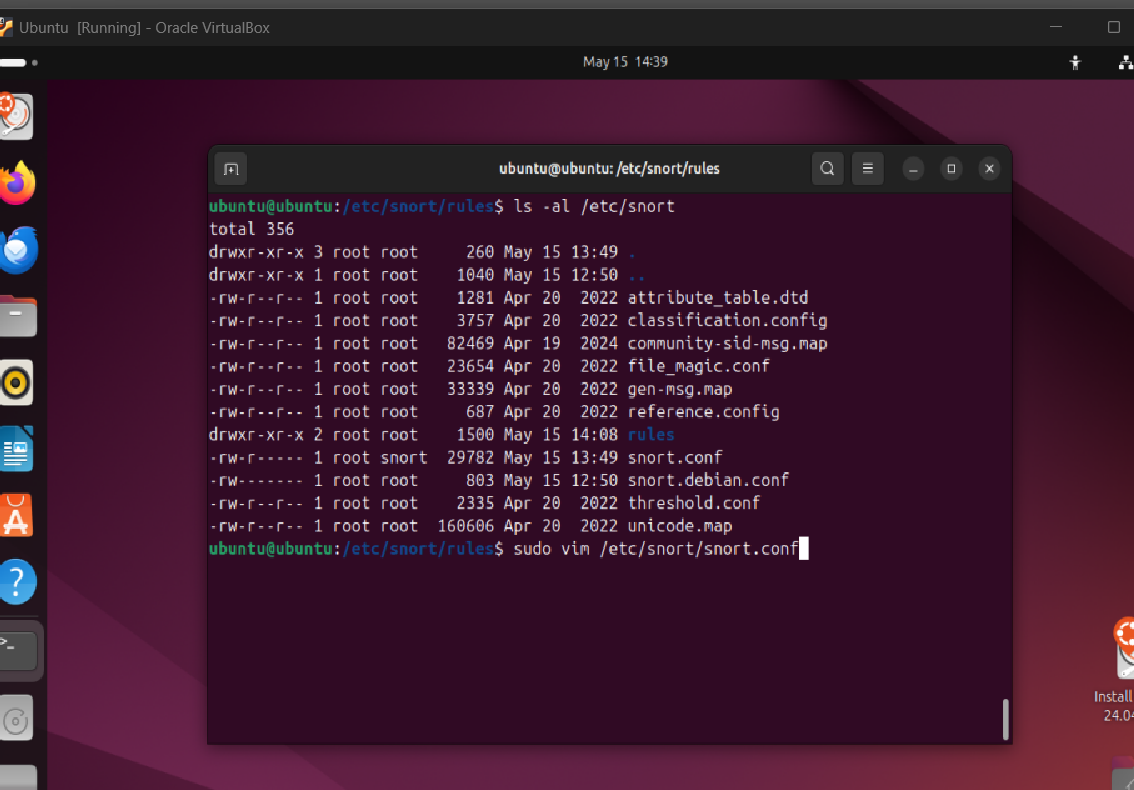
A screenshot of a computer

Description automatically generated

Now change all device network to Promiscuous mode and attach to Bridged Adapter.

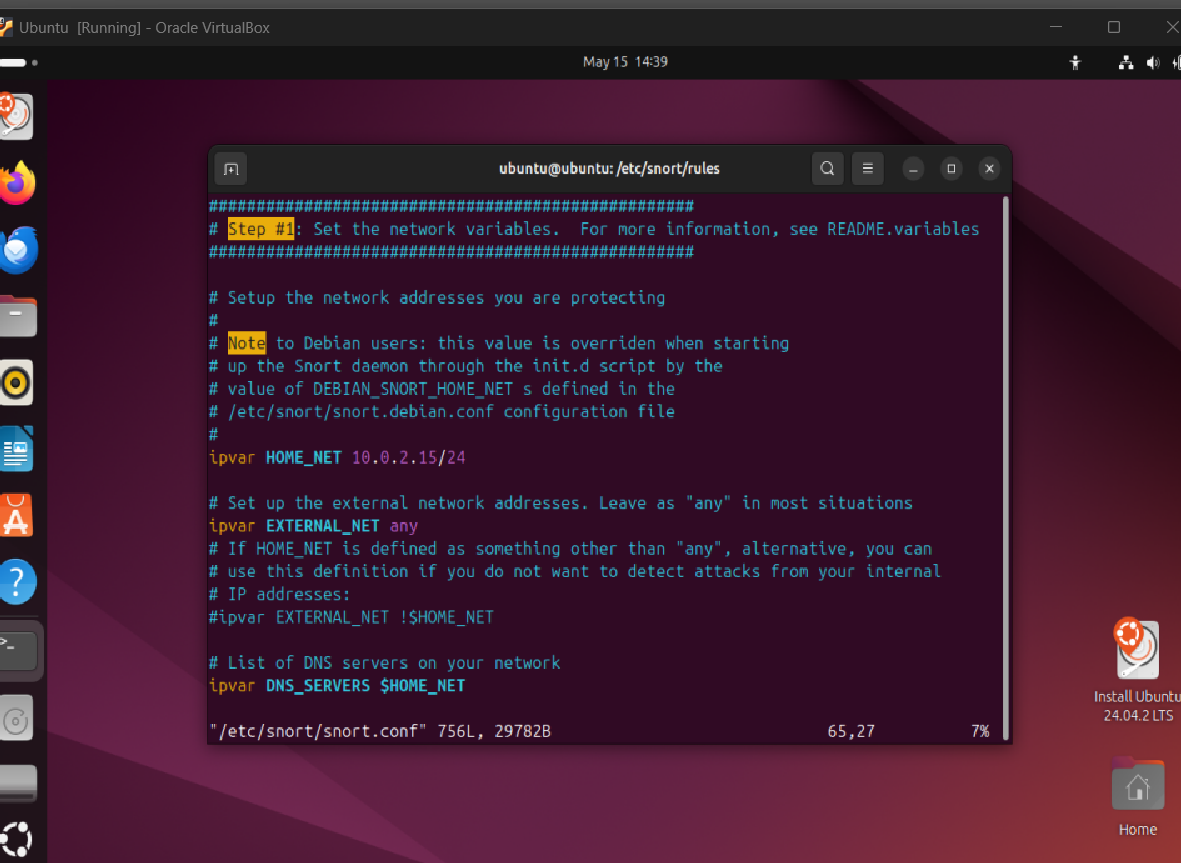
Step2: Install vim editor – sudo apt-get install vim

Go to the /etc/snort directory and then type in the following command to access snort.conf



Once inside the snort.conf, press I button to enter Insert mode then type in your local IP

next to the ipvar HOME\_NET and set EXTERNAL\_NET to any.



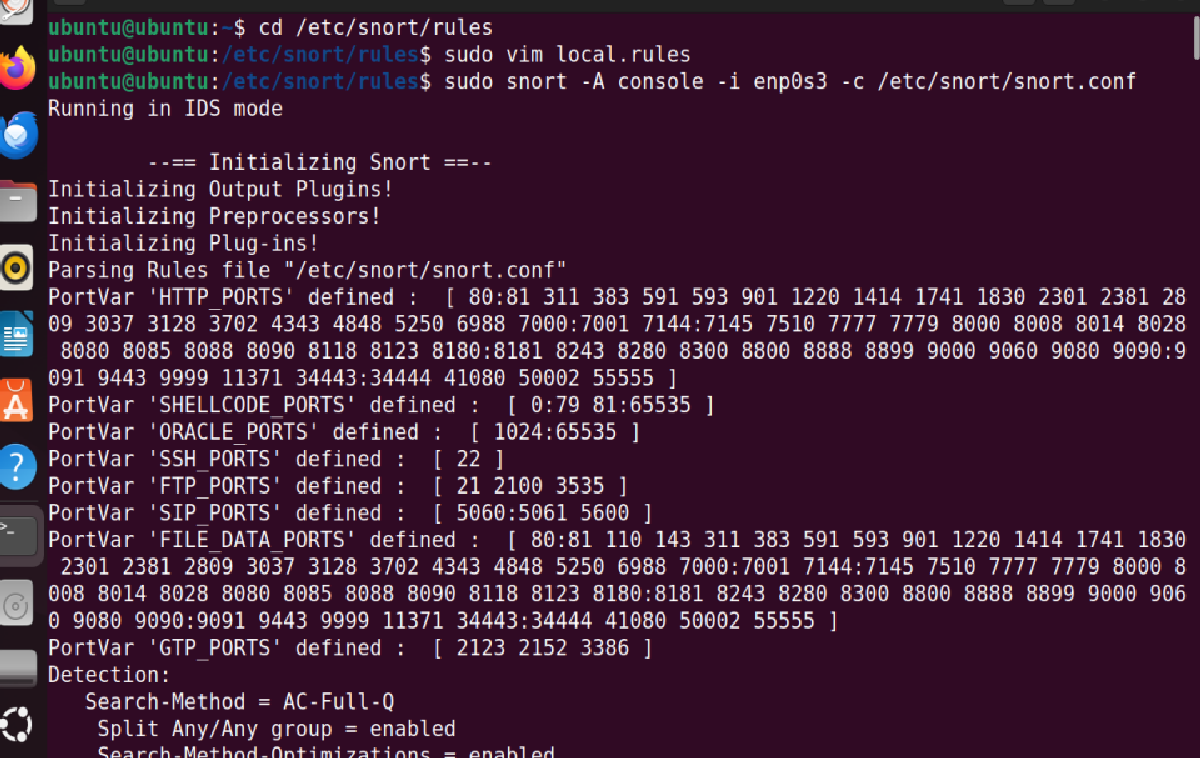
A screenshot of a computer

Description automatically generated

To get out of the vim editor press esc then Shift then wq, this will land us back to the terminal.

>sudo snort -A console -I enp0s3 -c /etc/snort/snort.conf

This will run a self-test mode in snort

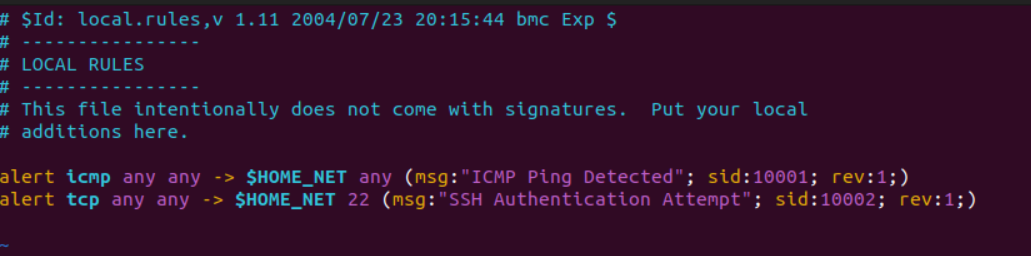


Step 3: Now to create our own rules in Snort we will go to the local.rules in the /etc/snort/rules directory.

A screenshot of a computer

Description automatically generated

This will Alert us if any ping request made from any external IP & external port into any device in our home subnet.



This will alert us if any SSH attempt is made from any external ip & external port into any device in our home subnet.

SNORPY

**Snorpy** is a **web-based Snort rule generator** designed to make writing Snort IDS rules easier. Snorpy provides a **form-based interface** where you can:

* Select protocol (TCP, UDP, ICMP, etc.)
* Define source and destination IPs and ports
* Add rule options like content, flags, flow, msg, sid, etc.
* Generate a valid Snort rule from your inputs

It takes care of:

* Proper rule formatting
* Syntax validation (to a degree)
* Reducing manual errors

**Example Use Case**

You want to detect outbound traffic to port 4444:

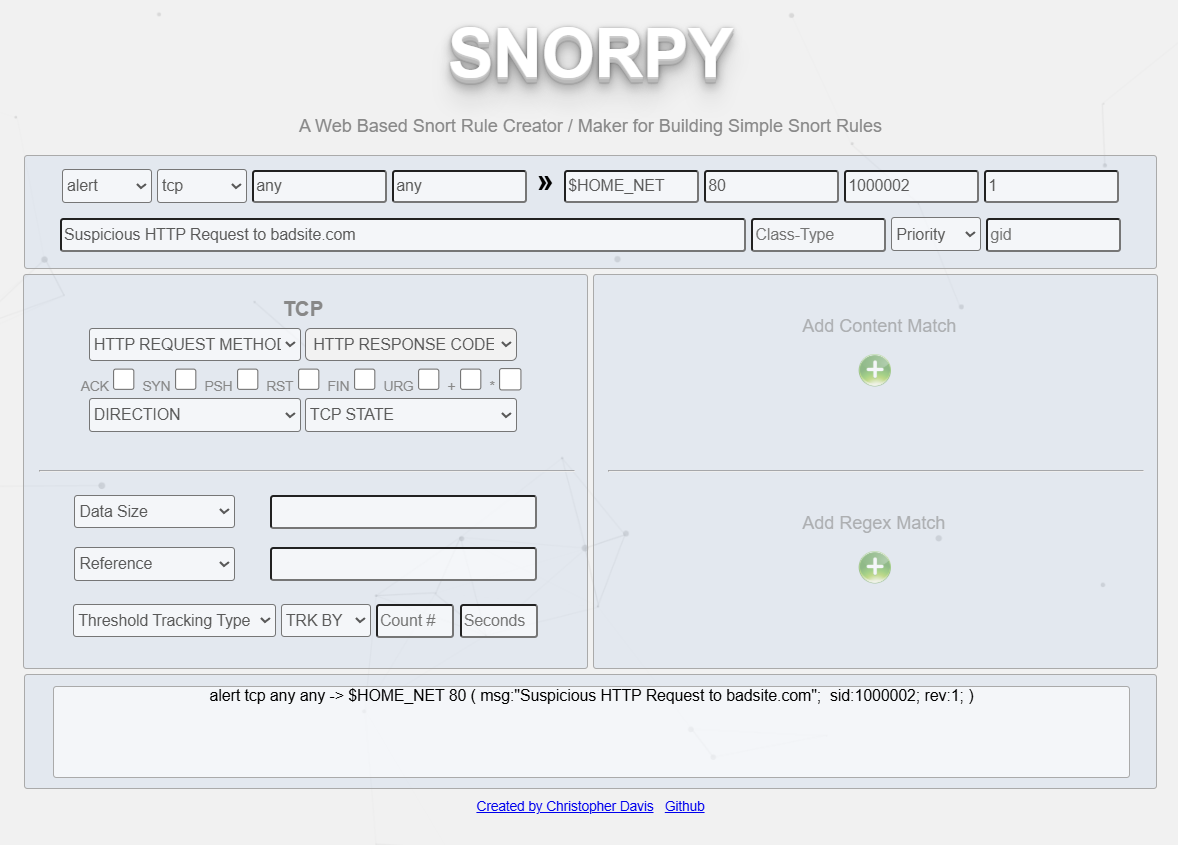
1. Go to Snorpy.
2. Choose TCP, source IP as $HOME\_NET, destination port as 4444.
3. Add a msg, give it a sid, and click "Generate."
4. Copy the rule Snorpy builds and paste it into your Snort config.

USING SNORPY TO CREATE Custom Rules

A screenshot of a computer

Description automatically generated

The above will give us a custom rule tailored to our needs we can create any no. of rules using SNORPY and use it in our own IDS.



Let’s say we want to detect an HTTP request to a suspicious domain badsite.com. So we can create it using SNORPY with much ease

alert tcp any any -> $HOME\_NET 80 ( msg:"Suspicious HTTP Request to badsite.com";  sid:1000002; rev:1; )